IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) An arrangement for blocking ~~of~~ unwanted network traffic in open data and telecommunication networks, ~~characterized by~~ comprising:

a first level of blocking ~~(350)~~ unwanted communications that contravene ordre public, said first level of blocking being in the form of a top level domain requiring registration for ~~web-sites (390)~~ websites residing within the top level domain ~~with respect to ordre public~~;

at least one top level domain server ~~(16)~~ for connection to the top level domain comprising or being connected to a domain name server ~~(14) files~~ file and software, which assign a ~~call~~ a network address to a~~, through~~ computer ~~(12)~~, ~~a~~ the network address ~~(340) which associates~~ associating the computer to ~~a correct~~ an application server ~~(380)~~ when ~~the~~ a user of the computer ~~(12)~~ has been identified;

database means ~~(18),~~ connected to the top level domain server ~~(16)~~ for ~~registration and approval of~~ registering and approving of a ~~services~~ service provider ~~(19)~~ residing within the top level domain;

means connected to or comprised in the top level domain server ~~(16)~~ for ~~identification of~~ identifying a calling ~~parties~~ party ~~identity (310)~~ during login to the top level domain;

means connected to or comprised in the top level domain server ~~(16)~~ for blocking ~~(330)~~ an unidentified calling party; ~~and~~

a second level of blocking providing micro debiting through a debiting server during connection to the top level domain, the second level of blocking including means for debiting of the top level domain via micro debiting and means for accumulating said micro debiting during every session a user is connected to said domain; and

a switch for use with the second level of blocking, the switch being adapted to be turned on and off based on debit-free time periods;

~~whereby~~ wherein registration of those connected to the top level domain and the identification of a calling party prevents a free connection and anonymity in computer networks through said top level domain server ~~(16), which accomplishes~~ so as to obtain a top level domain purged from unwanted network traffic.

2. (Cancelled).

3. (Currently Amended) An arrangement according to claim ~~2~~ 1, ~~characterized in that the~~ wherein the ~~web~~ network address of the ~~one connected (12)~~ computer is stored in a database for debiting ~~in a database (18)~~.

4. (Currently Amended) An arrangement according to claim ~~2 or~~ 3, ~~characterized by comprising:~~ wherein the debiting server comprises:

means ~~in the debiting server (20)~~ for ~~percentage partitions~~ partitioning ~~in at least two posts of~~ an accumulated micro ~~debitings~~ debiting into at least two posts for every session during login, ~~which~~ wherein the posts are credited to at least one of the top level domain and a registered service provider.

5. (Currently Amended) A method ~~relating to an arrangement~~ for blocking ~~of~~ unwanted network traffic in open data and telecommunication networks, ~~characterized by~~ comprising ~~the method steps of~~:

providing a first level of blocking ~~(350)~~ unwanted communications that contravene ordre public, said first level of blocking being in the form of a top level domain requiring registration for ~~web sites (390)~~ websites residing within the top level domain ~~with respect to ordre public~~;

connecting at least one top level domain server ~~(16) for connection~~ to the top level domain, the top level domain comprising or being connected to a domain name server ~~(14) files~~ file and software, which assign a network address to a ~~call, through~~ computer ~~(12)~~, ~~a~~ the network address ~~(340) which associates~~ associating the computer to ~~a correct~~ an application server ~~(380)~~ when ~~the~~ a user of the computer ~~(12)~~ has been identified;

connecting database means ~~(18), connected~~ to the top level domain server ~~(16)~~ for ~~registration and approval of~~ registering and approving of a ~~services~~ service provider ~~(19)~~ residing within the top level domain;

identifying a calling ~~parties~~ party ~~identity (320)~~ during login to the top level domain;

blocking ~~(330) through means for such a purpose of~~ an unidentified calling party; ~~and~~

providing a second level of blocking by (a) micro debiting the top level domain and (b) accumulating said micro debiting during every session a user is connected to said domain through a debiting server; and

executing micro debiting based on debit-free time periods;

~~whereby~~ wherein registration of those connected to the top level domain and the identification of a calling party prevents a free connection and anonymity in computer

networks through said top level domain server ~~(16),~~ so as to obtain ~~which accomplishes~~ a top level domain purged from unwanted network traffic.

6. (Cancelled).

7. (Currently Amended) A method ~~relating to an arrangement for blocking~~ according to claim ~~6~~ 5, ~~characterized in that~~ wherein the debiting includes storing the ~~web~~ network address of the ~~one connected (12)~~ computer ~~is stored for debiting~~ in a database ~~(18)~~.

8. (Currently Amended) A method ~~relating to an arrangement for blocking~~ according to claim ~~6 or~~ 7, wherein the micro debiting includes ~~characterized by comprising means in the debiting server (20) for percentage partitions~~ partitioning ~~in at least two posts of~~ an accumulated micro ~~debitings~~ debiting into at least two posts for every session during login, ~~which~~ wherein the posts are credited to at least one of the top level domain and a registered service provider.